Sums of normal endomorphisms. II

By R. H. BRUCK in Madison (Wisconsin, U. S. A.)[1])

Dedicated to L. Rédei on his sixtieth birthday

1. Introduction. The subject of this paper is (associative) rings of endomorphisms. However, the ring elements are not endomorphisms of groups but of loops, and the reader will need some acquaintance with loop theory — as given, for example, in [1].

Let G be any loop and let $\mathfrak{N}$ be the multiplicative semigroup of all normal endomorphisms of G (for the definition, see [1], [2] or [3]). Also let $\mathfrak{R}$ be the loop additively generated by $\mathfrak{N}$, where the operation is addition of single-valued mappings of G into G. In an earlier paper [3] of like title we found a necessary and sufficient condition (namely, power-associativity of G) in order that $\mathfrak{R}$ should be an associative ring (in the ordinary sense) with respect to addition and multiplication of mappings. However, $\mathfrak{R}$, even when it is a ring, need not consist only of endomorphisms (though see Theorem 6. 1 below) and, a fortiori, need not be contained in $\mathfrak{N}$.

In the present paper we are primarily concerned with rings contained wholly within $\mathfrak{N}$. The following result is typical:

The set $\mathfrak{N}$ of all normal endomorphisms of the loop G contains a unique maximal (associative) ring $\mathfrak{S}$, namely the set $\mathfrak{S}$ of all θ in $\mathfrak{N}$ such that $2\theta = \theta + \theta$ is also in $\mathfrak{N}$. (Theorem 5. 1.)

Clearly the defining condition for $\mathfrak{N}$ is a necessary condition that the element θ of $\mathfrak{N}$ be contained in a ring of elements of $\mathfrak{N}$. On the way toward Theorem 5. 1 we also prove the following (as a special case of Theorem 3. 2): *If θ, φ are in $\mathfrak{N}$, a necessary and sufficient condition that $\theta+\varphi$ be in $\mathfrak{N}$ is that $2\theta\varphi$ be in $\mathfrak{N}$* (that is, that $\theta\varphi$ be in $\mathfrak{S}$.)

When G is a group, the ring $\mathfrak{S}$ of Theorem 5. 1 is the ring of centralizing endomorphisms of G. When G is a loop, $\mathfrak{S}$ contains the ring of

[1]) The research for this paper was done in Frankfurt am Main, Germany, with the support of grants from the National Science Foundation, U. S. A., and from the Graduate Research Committee of the University of Wisconsin.

centralizing endomorphisms of G but can be much larger. Indeed, in § 4, as an essential part of our investigation, we consider *the loops G for which* $\mathfrak{S} = \mathfrak{N}$. One characterization of such loops (among several given in Theorem 4.1) is in terms of the following two conditions:

(i) *The mapping $x \to x^2x$ is a semi-normal endomorphism of G.*

(ii) *The mapping $x \to x^2$ is a semi-normal endomorphism of G which maps G into $C(G) \cap Z_2(G)$.*

(For the definitions of a *semi-normal* endomorphism, of the *Moufang centre*, $C(G)$, and of the *second centre*, $Z_2(G)$, of a loop G, see [2].)

It may be remarked that conditions (i), (ii) are satisfied, on the one hand, by the commutative Moufang loops which are centrally nilpotent of class at most two — a relatively restricted class, containing, however, all abelian groups — and, on the other hand, by the loops of exponent two — a large and as yet little known class of loops. (In this connection, see the remarks in § 4.) The latter class of loops turns up in another way, which we shall now explain.

Let $\mathfrak{N}'$ be the set of all strongly normal endomorphisms of the loop G. (For the definition and properties of $\mathfrak{N}'$, see [2]; we remark here that $\mathfrak{N}'$ is part, but not always all, of $\mathfrak{N}$, and that every element of N is a sum of two elements of $\mathfrak{N}'$.) Theorem 5.1 (quoted above) has an exact counterpart for $\mathfrak{N}'$:

The set $\mathfrak{N}'$ of all strongly normal endomorphisms of the loop G contains a unique maximal (associative) ring $\mathfrak{S}'$, namely the set $\mathfrak{S}'$ of all θ in $\mathfrak{N}'$ such that $2\theta = \theta + \theta$ is also in $\mathfrak{N}'$. (Theorem 5.2.)

When $\mathfrak{S}' = \mathfrak{N}'$, then $\mathfrak{S}' = \mathfrak{S} = \mathfrak{N}$. A necessary and sufficient condition that $\mathfrak{S}' = \mathfrak{N}'$ for a loop G is (see Theorem 4.2) that

(iii) *the mapping $x \to x^2$ of G is an endomorphism of G into its centre* $Z(G)$.

The condition (iii) implies, in particular, that $G/Z(G)$ is a loop of exponent two. A construction (in terms of central extensions) of the loops G satisfying (iii) is given at the end of § 4.

The methods of the paper take account of other possibilities. For example, if G is a Moufang (and hence power-associative) loop, it is shown in [2] that the ring $\mathfrak{N}$ of our second paragraph has the property that an endomorphism θ of G is in $\mathfrak{N}$ if and only if θ is semi-normal. Thus, in the case of an arbitrary loop G, the question arises as to what endomorphisms of G can be generated by normal endomorphisms of G. As a start on this question, we determine necessary and sufficient conditions that the sum, $\theta + \varphi$, of two normal endomorphisms θ, φ of G should be an endomorphism of G (Theorem 2. 1) and should be semi-normal, weakly normal or normal (Theorem 3. 1). In each case, $\theta+\varphi$ has the same "type" as $2\theta\varphi$. Thus, for example, *the loops for which the sum of every two normal endomorphisms is an endomorphism are precisely those satisfying the identical relation*

$$(1.1) \qquad (xy)^2 = x^2y^2.$$

And $\theta+\varphi$ is an endomorphism of the loop G (for θ, φ normal endomorphisms of G) precisely when $G\theta\varphi$ satisfies the identical relation (1. 1).

Let us mention here a special class of loops satisfying (1. 1). If the loop G is *di-associative* (that is, if every two elements of G generate a group) then (1. 1) holds precisely when G is commutative. On the other hand, if G is commutative and di-associative, and if $\mathfrak{R}$ is the ring of our second paragraph, then $\mathfrak{R}$ consists entirely of endomorphisms (Theorem 6. 1). But, without further hypotheses, we are unable to say much about the nature of the endomorphisms in $\mathfrak{R}$.

At the present time we have no adequate tools for studying the class of all loops satisfying (1. 1). Consequently, in § 4, we impose additional hypotheses. In Lemma 4. 1 we assume that the mapping $x\to x^2$ of the loop G is a semi-normal endomorphism. Then G is power-associative and the commutator-associator subloop, G', has exponent dividing six. If we assume still further (to give one of several equivalent conditions) that the mapping $x\to x^3$ is a semi-normal endomorphism, then (Lemma 4. 3) every power-mapping $(n): x\to x^n$, is a semi-normal endomorphism of G. Moreover, (n) is centralizing if $n\equiv 0 \bmod 6$, (n) is strongly normal if $n\equiv 0$ or $1 \bmod 3$, and (n) has the same "type" as (2) if $n\equiv 2 \bmod 3$. — All of these conclusions are true (in slightly stronger form) for arbitrary commutative Moufang loops but not (I believe) for arbitrary commutative di-associative loops. — The conditions that (2) be normal or strongly normal (given in Lemma 4. 3) then lead to the characterizations, given above, of the loops G for which $\mathfrak{S}=\mathfrak{N}$ or $\mathfrak{S}'=\mathfrak{N}'$.

We shall end this introduction with an unsolved problem. It seems likely that if G is a (necessarily) power-associative loop all of whose power-mappings are semi-normal endomorphisms, then the ring $\mathfrak{R}$ generated by the normal endomorphisms consists entirely of endomorphisms, and probably of semi-normal endomorphisms.

2. The word f_4. We define the loop word f_4 as follows:

$$(2.1) \qquad (X_1X_2)(X_3X_4) = [(X_1X_3)(X_2X_4)]\cdot f_4(X_1, X_2, X_3, X_4).$$

As pointed out in [2], the word f_4 is important in the study of sums of endomorphisms. Specifically, Lemma 3. 1 of [2] can be phrased as follows:

Lemma 2.1. *Let θ, φ, ψ be single-valued mappings of a loop G into itself, such that*

(i) $\theta+\varphi=\psi$;

(ii) *some two of θ, φ, ψ are endomorphisms of G.*

A necessary and sufficient condition that the remaining mapping be an endomorphism of G is that

$$f_4(x\theta, x\varphi, y\theta, y\varphi)=1 \tag{2.2}$$

for all x, y in G.

The word f_4 is purely non-abelian but not normalized. (For the definition of these terms, see [2].) Our first step here is to express f_4 in terms of normalized, purely non-abelian loop words. In addition to the commutator-word, (X_1, X_2), and the associator-word, (X_1, X_2, X_3), we need a second type of associator-word, A, and three additional words, g_3, h_3, k_4. The definitions are as follows, in terms of an auxiliary word P:

$$X_1X_2=[X_2X_1]\cdot(X_1, X_2), \tag{2.3}$$

$$(X_1X_2)X_3=[X_1(X_2X_3)]\cdot(X_1, X_2, X_3), \tag{2.4}$$

$$X_1(X_2X_3)=[(X_1X_2)X_3]\cdot A(X_1, X_2, X_3), \tag{2.5}$$

$$(X_1X_2)X_3=[(X_1X_3)X_2][(X_2, X_3)\cdot g_3(X_1, X_2, X_3)], \tag{2.6}$$

$$X_1(X_2X_3)=[X_2(X_1X_3)][(X_1, X_2)\cdot h_3(X_1, X_2, X_3)], \tag{2.7}$$

$$\begin{aligned} &f_4(X_1, X_2, X_3, X_4)=\\ &=[(X_2, X_3)\cdot g_3(X_1, X_2, X_3)][(X_1, X_2, X_4)\cdot P(X_1, X_2, X_3, X_4)], \end{aligned} \tag{2.8}$$

$$P(X_1, X_2, X_3, X_4)=A(X_1, X_3, X_4)\cdot[h_3(X_2, X_3, X_4)\cdot k_4(X_1, X_2, X_3, X_4)]. \tag{2.9}$$

Here (2.8), (2.9) together express f_4 in terms of the commutator and associator words and the words A, g_3, h_3, k_4. That the commutator and associator words, together with A, are both purely non-abelian and normalized is evident from (2.3), (2.4), (2.5). From (2.6), (2.7), g_3 and h_3 are certainly purely non-abelian. To see that they are normalized, we need only note that they vanish (i.e., take the value 1) when any one of X_1, X_2, X_3 is replaced by 1. Next we compare (2.1), (2.8). Since f_4, g_3 are purely non-abelian, so is P. Therefore, by (2.9), k_4 is also purely non-abelian. To see that k_4 is normalized, we proceed as follows: In (2.1) we replace X_4, X_3, X_2, X_1 in turn by 1 and compare with (2.6), (2.4), (2.5), (2.7) respectively, getting

$$\begin{gathered} f_4(X_1, X_2, X_3, 1)=(X_2, X_3)\cdot g_3(X_1, X_2, X_3),\\ f_4(X_1, X_2, 1, X_4)=(X_1, X_2, X_4), \qquad f_4(X_1, 1, X_3, X_4)=A(X_1, X_3, X_4),\\ f_4(1, X_2, X_3, X_4)=(X_2, X_3)\cdot h_3(X_2, X_3, X_4). \end{gathered} \tag{2.10}$$

From (2.10) in (2.8) we get

$$
\begin{aligned}
&P(X_1, X_2, X_3, 1) = 1,\\
&P(X_1, X_2, 1, X_4) = 1,\\
(2.11)\qquad &P(X_1, 1, X_3, X_4) = A(X_1, X_3, X_4),\\
&P(1, X_2, X_3, X_4) = h_3(X_2, X_3, X_4).
\end{aligned}
$$

And (2.11), (2.9) show us that k_4 is normalized. To sum up:

Lemma 2.2. *The commutator and associator words, and the words A, g_3, h_3, k_4 are normalized, purely non-abelian loop words, and f_4 is expressible (by (2.8), (2.9)) as a product in these words.*

Remark. The words A, g_3, h_3, k_4 were found from f_4 by applying the method, described in [3], of expressing a purely non-abelian word in terms of essentially normalized purely non-abelian words.

Our first use of the formula just discussed is to prove the following:

Lemma 2.3. *Let θ, φ be normal endomorphisms of the loop G. Then, for all x, y in G,*

$$(2.12)\qquad f_4(x\theta, x\varphi, y\theta, y\varphi) = f_4(x, x, y, y)\theta\varphi,$$

$$(2.13)\qquad f_4(x, x, y, y)\theta = f_4(x, x, y, y)\theta^2,$$

$$(2.14)\qquad f_4(x, x, y, y)\theta\varphi = f_4(x, x, y, y)\varphi\theta.$$

Proof. Since the formula obtained from (2.8), (2.9) by eliminating P is too long to be displayed conveniently, our proof will be given in slightly imprecise terms. These the reader should be able to interpret correctly.

Substituting $x\theta, x\varphi, y\theta, y\varphi$ for X_1, X_2, X_3, X_4 respectively in (2.8), (2.9), we see that the left-hand side of (2.12) is a (precisely defined) product of the following:

$$
\begin{aligned}
&(x\varphi, y\theta) = (x, y)\theta\varphi,\\
&g_3(x\theta, x\varphi, y\theta) = g_3(x, x, y)\theta^2\varphi,\\
&(x\theta, x\varphi, y\varphi) = (x, x, y)\theta\varphi^2,\\
(2.15)\qquad &A(x\theta, y\theta, y\varphi) = A(x, y, y)\theta^2\varphi,\\
&h_3(x\varphi, y\theta, y\varphi) = h_3(x, y, y)\theta\varphi^2,\\
&k_4(x\theta, x\varphi, y\theta, y\varphi) = k_4(x, x, y, y)\theta^2\varphi^2.
\end{aligned}
$$

To prove (2.12) we need only show that, on the right-hand sides of the equations in (2.15), each of $\theta^2\varphi$, $\theta\varphi^2$ and $\theta^2\varphi^2$ has the same effect as $\theta\varphi$. The method is the same in each case, and we treat only one example.

The word W_2 defined by

$$W_2(X, Y) = g_3(X, X, Y)$$

is normalized and purely non-abelian. Thus, since θ is a normal endomorphism, we have, for all x, y in G,

$$W_2(x, y)\theta = W_2(x\theta, y\theta) = W_2(x, y)\theta^2.$$

Similarly, since θ and φ are normal endomorphisms,

$$W_2(x, y)\theta\varphi = W_2(x\theta, y\varphi) = W_2(x, y)\varphi\theta.$$

This is enough — since the normal endomorphisms form a multiplicative semigroup — to indicate how to complete the proof of Lemma 2. 3.

The next lemma is mainly included as a simple application of Lemma 2. 3. We recall that a loop G is *di-associative* if, for every two elements x, y of G, the subloop generated by x and y is a group.

Lemma 2. 4. *Let θ, φ be normal endomorphisms of the loop G such that the subloop $G\theta\varphi$ is commutative and di-associative. Then $\theta + \varphi = \varphi + \theta$ is an endomorphism of G.*

Proof. For any x in G, $(x\theta, x\varphi) = (x, x)\theta\varphi = 1$; and this implies that $\theta + \varphi = \varphi + \theta$. By two applications of (2. 12),

$$f_4(x\theta, x\varphi, y\theta, y\varphi) = f_4(x\theta\varphi, x\theta\varphi, y\theta\varphi, y\theta\varphi) = 1,$$

the last step following directly from (2. 1) and the fact that $x\theta\varphi, y\theta\varphi$ lie in an abelian group. Consequently, by Lemma 2. 1, $\theta + \varphi$ is an endomorphism of G.

We shall need two more lemmas concerning f_4.

Lemma 2. 5. *If θ is a normal endomorphism of the loop G, then*

$$f_4(x\theta, x\theta, y\theta, z\theta) = f_4(x\theta, x\theta, y, z) \tag{2. 16}$$

for all x, y, z in G.

Proof. The proof is very similar to that of Lemma 2. 3. To save space, we list below the six terms of which the left-hand side of (2. 16) is a product, and transform these into six terms of which the right-hand side of (2. 16) is a similar product:

$$\begin{aligned}(x\theta, y\theta) &= (x, y)\theta = (x\theta, y),\\ g_3(x\theta, x\theta, y\theta) &= g_3(x, x, y)\theta = g_3(x\theta, x\theta, y),\\ (x\theta, x\theta, z\theta) &= (x, x, z)\theta = (x\theta, x\theta, z),\\ A(x\theta, y\theta, z\theta) &= A(x, y, z)\theta = A(x\theta, y, z),\\ h_3(x\theta, y\theta, z\theta) &= h_3(x, y, z)\theta = h_3(x\theta, y, z),\\ k_4(x\theta, x\theta, y\theta, z\theta) &= k_4(x, x, y, z)\theta = k_4(x\theta, x\theta, y, z).\end{aligned} \tag{2. 17}$$

Here we need to make some remarks. In each of the formulas (2. 17), the left-hand term is equal to the middle term merely on the ground that θ is an endomorphism of G. In the case of the first, fourth and fifth formulas of (2. 17), we get from the middle term to the ringht-hand term by straightforward use of the normality of θ. For the second, third and sixth formulas a slight variation is necessary. If W_2 is defined by

$$W_2(X, Y) = g_3(X, X, Y),$$

then W_2 is normalized and purely non-abelian. Hence

$$g_3(x, x, y)\theta = W_2(x, y)\theta = W_2(x\theta, y) = g_3(x\theta, x\theta, y).$$

Similarly in the remaining cases. This proves Lemma 2. 5.

At this point we recall that the *Moufang centre*, $C(G)$, of a loop G, consists of all a in G such that

$$(aa)(yz) = (ay)(az) \tag{2.18}$$

for all y, z in G. It is shown in [2] that $C(G)$ is a (commutative, Moufang) subloop of G and that $C(G)$ has an important rôle in the theory of normal endomorphisms.

Lemma 2. 6. *Let θ be a normal endomorphism of the loop G and let a be an element of G. Then each of the following statements implies the other:*

(i) *$a\theta$ lies in the Moufang centre $C(G\theta)$ of $G\theta$.*

(ii) *$a\theta$ lies in the Moufang centre $C(G)$ of G.*

Proof. We note, in view of (2. 1), that (2. 18) is equivalent to

$$f_4(a, a, y, z) = 1. \tag{2.19}$$

On the other hand, by Lemma 2. 5,

$$f_4(a\theta, a\theta, y\theta, z\theta) = f_4(a\theta, a\theta, y, z). \tag{2.20}$$

Thus (i) holds precisely when the left side of (2. 20) vanishes for all y, z in G; and (ii) holds precisely when the right side of (2. 20) vanishes for all y, z in G. This completes the proof of Lemma 2. 6.

Now we are ready for some initial theorems. From Lemma 2. 3 we deduce the following:

Theorem 2. 1. *Let θ, φ be normal endomorphisms of the loop G. Then each of the following statements implies the other two:*

(i) *$\theta + \varphi$ is an endomorphism of G.*

(ii) *$2\theta\varphi = \theta\varphi + \theta\varphi$ is an endomorphism of G.*

(iii) *If α, β are elements of the multiplicative semigroup generated by θ, φ and the identity mapping of G, and if $\alpha\beta$ contains each of θ and φ as a factor, then $\alpha+\beta$ is an endomorphism of G.*

Proof. The hypotheses on α and β in (iii) ensure that α and β are normal endomorphisms of G. Hence, by Lemma 2.3,

$$f_4(x\alpha, x\beta, y\alpha, y\beta) = f_4(x, x, y, y)\alpha\beta. \tag{2.21}$$

Since $\alpha\beta$ is a product formed from θ and φ, and contains each of θ and φ as a factor, then, by Lemma 2.3 again,

$$f_4(x, x, y, y)\alpha\beta = f_4(x, x, y, y)\theta\varphi.$$

Therefore the left-hand side of (2.21) is independent of the particular choice of α and β. In particular, $\alpha=\theta, \beta=\varphi$ and $\alpha=\beta=\theta\varphi$ are two admissible choices for α, β; another is $\alpha=1, \beta=\varphi\theta$, for example. However, by Lemma 2.1, a necessary and sufficient condition that $\alpha+\beta$ be an endomorphism of G is that

$$f_4(x\alpha, x\beta, y\alpha, y\beta) = 1$$

for all x, y in G. This completes the proof of Theorem 2.1.

As a corollary of Theorem 2.1 we obtain the following:

Theorem 2.2. *Let G be a loop, let $\mathfrak{N}$ be the set of all normal endomorphisms of G, and let $\mathfrak{S}^*$ be the set of all θ in $\mathfrak{N}$ such that $2\theta = \theta+\theta$ is an endomorphism of G. Then each of the following statements implies all the others:*

(i) *θ is in $\mathfrak{S}^*$.*

(ii) *θ is in $\mathfrak{N}$ and $1+\theta$ is an endomorphism of G.*

(iii) *$\theta\mathfrak{N} \subset \mathfrak{S}^*$.*

(iv) *$\mathfrak{N}\theta \subset \mathfrak{S}^*$.*

(v) *$\theta \in \mathfrak{N}$, and $\theta+\varphi, \varphi+\theta$ are endomorphisms of G for every θ in $\mathfrak{N}$.*

Proof. Let θ, φ be in $\mathfrak{N}$. By Theorem 2.1, if one of $\theta+\varphi$, $\varphi+\theta$, $2\theta\varphi$, $2\varphi\theta$ is an endomorphism of G, all are. Taking $\varphi=1$, we see the equivalence of (i), (ii). We also see that each of (iii), (iv), (v) implies (i). Keeping φ general, we see that (i) implies (iii), (iv) and (v). This completes the proof of Theorem 2.2.

There is still another corollary of interest:

Theorem 2.3. *Let G be a loop. Then a necessary and sufficient condition that the sum of every two normal endomorphisms of G be an endomorphism of G is that the square-mapping (2), defined by*

$$x(2) = x^2, \quad \textit{all } x \in G, \tag{2.22}$$

be an endomorphism of G; that is, that G satisfy the identical relation

$$(xy)^2 = x^2y^2. \tag{2.23}$$

Proof. In the notation of Theorem 2.2, $\mathfrak{S}^* = \mathfrak{N}$ if and only if the identity mapping 1 is in $\mathfrak{S}^*$. And 1 is in $\mathfrak{S}^*$ if and only if the mapping (2) is an endomorphism of G.

Remark. If θ is an endomorphism of a loop G,

$$\theta(2) = (2)\theta = 2\theta.$$

Hence the study of the $\mathfrak{S}^*$ of Theorem 2.2 is equivalent to the study of those normal endomorphisms θ of G with the property that the sum of every two normal endomorphisms of $G\theta$ is an endomorphism of $G\theta$.

3. Normality of sums. In studying the question of "normality" of a given endomorphism θ of a loop G, we have to consider the validity of equations of the type

$$W_n(x_1\theta, x_2, \ldots, x_n) = W_n(x_1, x_2, \ldots, x_n)\theta, \tag{3.1}$$

required to hold for all $x_1, \ldots, x_n$ in G. Here W_n is a normalized purely non-abelian word. For θ to be normal, (3.1) must hold for all choices of W_n. For θ to be weakly normal or semi-normal, (3.1) must hold for choices of W_n prescribed by the definitions. (See [2].)

In view of Theorems 2.1, 2.2, the next lemma seems natural. We suppose given a normalized, purely non-abelian word W_n. Then the word $F = F_{n+1}$, defined by

$$\begin{aligned} W_n(XY, Z_2, \ldots, Z_n) = \\ = [W_n(X, Z_2, \ldots, Z_n)\, W_n(Y, Z_2, \ldots, Z_n)]\, F(X, Y, Z_2, \ldots, Z_n), \end{aligned} \tag{3.2}$$

is also normalized and purely non-abelian.

Lemma 3.1. *Let θ, φ be normal endomorphisms of the loop G. Let α, β be elements of the multiplicative semigroup generated by θ, φ and the identity mapping of G, such that $\alpha\beta$ contains both θ and φ as factors. Then, for all $x, z_2, \ldots, z_n$ in G,*

$$\begin{aligned} W_n(x(\alpha+\beta), z_2, \ldots, z_n) = \\ = [W_n(x, z_2, \ldots, z_n)(\alpha+\beta)]\,[F(x, x, z_2, \ldots, z_n)\theta\varphi]. \end{aligned} \tag{3.3}$$

Proof. We recall that if a is any element of the commutator-associator subloop, G', of G, then

$$a\theta = a\theta^3, \quad a\theta\varphi = a\varphi\theta$$

for all normal endomorphisms θ, φ of G. Again, if $x, y, z_2, \ldots, z_n$ are arbitrary elements of G, the elements

$$a = W_n(x, z_2, \ldots, z_n), \quad b = F(x, y, z_2, \ldots, z_n)$$

are in G'. Since

$$a\theta = W_n(x, z_2, \ldots, z_n)\theta = W_n(x\theta, z_2\theta, \ldots, z_n\theta) = a\theta^n,$$

we see from (3. 2) that

$$b\theta = b\theta^n.$$

But, equally, since $F = F_{n+1}$,

$$b\theta = b\theta^{n+1}.$$

Since one of $n, n+1$ is even, and since

$$b\theta^2 = b\theta^4,$$

we deduce that

$$b\theta = b\theta^2$$

for every normal endomorphism θ. Thus also, if α, β are defined as in Lemma 3. 1,

$$b\alpha\beta = b\theta\varphi.$$

As a particular case of this we have

(3. 4) $\quad F(x\alpha, x\beta, z_2, \ldots, z_n) = F(x, x, z_2, \ldots, z_n)\,\alpha\beta = F(x, x, z_2, \ldots, z_n)\,\theta\varphi.$

Now we substitute $x\alpha, x\beta, z_2, \ldots, z_n$ for $X, Y, Z_2, \ldots, Z_n$ respectively in (3, 2), note that $(x\alpha)(x\beta) = x(\alpha+\beta)$, and use (3. 4). The result is (3. 3). This completes the proof of Lemma 3. 1.

Combining Lemma 3. 1 with Theorem 2. 1, we get the following:

Theorem 3. 1. *Let θ, φ be normal endomorphisms of the loop G. Let α, β be elements of the multiplicative semigroup generated by θ, φ and the identity mapping of G, such that $\alpha\beta$ contains both θ and φ as factors. If any one of $\theta+\varphi$, $2\theta\varphi$, $\alpha+\beta$ is a semi-normal (or weakly normal, or normal) endomorphism of G, then all are.*

As a special case (cf. the proof of Theorem 2. 2):

Theorem 3. 2. *Let $\mathfrak{N}$ be the set of all normal endomorphisms of the loop G. Let P be any fixed one of the properties of being a semi-normal, weakly normal or normal endomorphism of G. Let $\mathfrak{S}(P)$ be the set of all θ in $\mathfrak{N}$ such that $2\theta = \theta + \theta$ has property P. Then each of the following statements implies all the others:*

(i) $\theta \in \mathfrak{S}(P)$.

(ii) $\theta \in \mathfrak{N}$, *and* $1+\theta$ *has property* P.

(iii) $\theta\mathfrak{N}\subset\mathfrak{S}(P)$.

(iv) $\mathfrak{N}\theta\subset\mathfrak{S}(P)$.

(v) *$\theta\in\mathfrak{N}$, and $\theta+\varphi$, $\varphi+\theta$ have property P for every $\varphi\in\mathfrak{N}$.*

As another special case (cf. the proof of Theorem 2.3):

Theorem 3.3. *Let G be a loop. If the square-mapping, (2), of G is a semi-normal, weakly normal or normal endomorphism of G, then (and only then) the sum of every two normal endomorphisms of G has the corresponding property.*

4. The square-mapping. Theorems 2.2, 2.3 suggest that we consider next a loop satisfying the identical relation

$$(4.1)\qquad (xy)^2=x^2y^2,$$

which means that the square-mapping (2): $x\to x^2$ is an endomorphism. However, we shall impose the stronger conditions appropriate to Theorems 3.2, 3.3.

Lemma 4.1. *Let the square-mapping (2) be a semi-normal endomorphism of the loop G. Then:*

(i) *G is power-associative;*

(ii) *the commutator-associator subloop G' has exponent dividing six;*

(iii) *G satisfies the identical relations*

$$(4.2)\qquad (x^2,y)=(x,y)^2=1,$$

$$(4.3)\qquad (x^2,y,x)=(x,y^2,x)=(x,y,x^2)=(x,y,x)^2=1,$$

$$(4.4)\qquad (x^2,y,z)^3=(x,y^2,z)^3=(x,y,z^2)^3=(x,y,z)^6=1.$$

Proof. The main difficulty is the proof of (i), and for this we need neither (ii) nor the identity (4.4). Hence we begin by temporarily assuming (i). We recall that a loop is power-associative if each subloop which can be generated by one element is a (cyclic) group.

Assume (i) and set $\theta=(2)$. Then (see [2]) θ and θ^3 coincide on G'. Consequently, $a^2=a^8$ for each a in G'. Thus $a^6=1$, proving (ii). Since (2) is semi-normal and (x,y,z) is in G', formula (4.4) now follows immediately.

Now we are ready to prove (i). For each x in G and for each integer n (positive, negative or zero) we define the *right powers* x^n inductively by

$$(4.5)\qquad x^0=1,\quad x^nx=x^{n+1}.$$

In particular, $x^1=x$, $x^2=xx$. To prove (4.2), we note that

$$(x^2,y)=(x,y)^2=(x^2,y^2)=(x^2,y)^2=(x^2,y)(x^2,y)$$

and hence

$$1=(x^2,y)=(x,y)^2.$$

In view of (4.2),

$$(x^2y)x^2 = x^2(x^2y) = x^2(yx^2)$$

and hence

$$(x^2, y, x^2) = 1.$$

Therefore

$$(x, y, x)^2 = (x^2, y^2, x^2) = (x^2, y, x^2)^2 = 1.$$

From this, (4.3) follows immediately.

Next we need the formula

$$x^n x^2 = x^{n+2} \tag{4.6}$$

for every integer n. Since (4.6) is trivial for $n=0$, we assume inductively that (4.6) holds for some n. First we choose y so that

$$yx^2 = x^{n+1}.$$

By this with (4.6), (4.5), (4.2), (4.3),

$$x^n x^2 = x^{n+2} = x^{n+1}x = (yx^2)x = (x^2y)x = x^2(yx) = (yx)x^2.$$

Thus

$$yx = x^n, \quad y = x^{n-1}.$$

Hence (4.6) holds for $n-1$. Again, by (4.5), (4.6),

$$(x^n x)x = x^{n+2} = x^n x^2 = x^n(xx),$$

whence

$$(x^n, x, x) = 1$$

and, by (4.3),

$$(x^n, x^2, x) = (x^n, x, x^2) = (x^n, x, x)^2 = 1.$$

The latter formulas, along with (4.6), (4.2), yield

$$x^{n+3} = x^{n+2}x = (x^n x^2)x = x^n(x^2x) = x^n(xx^2) = (x^n x)x^2 = x^{n+1}x^2.$$

Thus (4.6) also holds for $n+1$, and the inductive proof of (4.6) is complete.

We observe that

$$x^{2n} = (x^2)^n \tag{4.7}$$

is true for $n=0$. Moreover, for every n,

$$x^{2n}x^2 = x^{2(n+1)},$$

$$(x^2)^n x^2 = (x^2)^{n+1},$$

by (4.6) and (4.5) respectively. Therefore (4.7) holds for every n.

Since (2) is an endomorphism, the right-hand side of (4.7) is a square. Thus

$$x^{2n} = (x^n)^2, \quad (x^{2n}, y) = 1 \tag{4.8}$$

for all x, y in G and all integers n. By (4.8),

$$x^n x = x x^n \tag{4.9}$$

when n is an even integer. When $n = 2k+1$, (4.8), (4.3) yield

$$x^n x = x^{2k+1} x = (x^{2k} x) x = (x x^{2k}) x = x(x^{2k} x) = x x^n.$$

Therefore (4.9) holds for all n. In particular,

$$x^{-1} x = 1 = x x^{-1}, \quad (x^{-1})^{-1} = x. \tag{4.10}$$

To begin with, we prove the next formula for non-negative n:

$$x^n x^{-1} = x^{n-1}. \tag{4.11}$$

This is trivial for $n = 0$; true for $n = 1$ by (4.10); and true for $n = 2$ by (4.6) (with $n = -1$) and (4.2). We need these special cases for the proof. If (4.11) holds for some $n \geqq 2$, then

$$x^{n-1} = x^n x^{-1} = (x^{n-1} x) x^{-1} = [x^{n-1}(x x^{-1})](x^{n-1}, x, x^{-1}) = x^{n-1}(x^{n-1}, x, x^{-1}).$$

The associator clearly must be 1. Thus

$$(x^{n-1}, x^2, x^{-1}) = (x^{n-1}, x, x^{-1})^2 = 1$$

and hence, by use of (4.6),

$$x^{n+1} x^{-1} = (x^{n-1} x^2) x^{-1} = x^{n-1}(x^2 x^{-1}) = x^{n-1} x = x^n.$$

This proves (4.11) for all $n \geqq 0$. From (4.11) we deduce the formula

$$(x^{-1})^{-n} = x^n \tag{4.12}$$

as follows: Certainly (4.12) holds for $n = 0$. If (4.12) holds for some $n \geqq 0$, then (setting $y = x^{-1}$ for convenience) we use (4.12), (4.11) to get

$$y^{-n-1} y = y^{-n} = x^n = x^{n+1} y,$$

whence we see that (4.12) holds for $n+1$. Hence (4.12) holds for all $n \geqq 0$. However, on replacing x in (4.12) by its inverse, and using (4.10), we get

$$x^{-n} = (x^{-1})^n,$$

which shows that (4.12) also holds for all negative n. — At this point we could go back and prove (4.11) for all negative n, but we do not need to do so.

Now we are ready to prove the main formula:

$$x^m x^n = x^{m+n}. \tag{4.13}$$

When we say that (4.13) holds for $n = k$, we mean that (4.13) holds for $n = k$ when m takes on all integral values. Certainly (4.13) holds for $n = 0$ and $n = 1$. Moreover, (4.13) holds for $n = 2$ by (4.8). Thus we consider some integer $k \geqq 1$ and assume inductively that (4. 13) holds for $0 \leqq n \leqq 2k$. In particular, since $k+1 \leqq 2k$, (4. 13) holds for $n=k$, $n=k+1$. Thus, for every integer m,

$$(x^m x^k)x = x^{m+k}x = x^{m+k+1} = x^m x^{k+1} = x^m(x^k x),$$

so that $(x^m, x^k, x) = 1$ and therefore, by (4. 8), on successive squaring,

$$(x^m, x^{2k}, x) = 1 = (x^m, x^{2k}, x^2).$$

By the latter formulas and the inductive assumption,

$$x^m x^{2k+1} = x^m(x^{2k}x) = (x^m x^{2k})x = x^{m+2k}x = x^{m+2k+1}$$

and

$$x^m x^{2k+2} = x^m(x^{2k}x^2) = (x^m x^{2k})x^2 = x^{m+2k}x^2 = x^{m+2k+2}.$$

Therefore (4. 13) holds for $n=2k+1$, $n=2k+2$ and hence for every non-negative n. To obtain (4. 13) for negative n, we simply replace x in (4. 13) by x^{-1} and use (4. 12). This completes the proof of (4. 13). Since (4. 13) implies (i), the proof of Lemma 4. 1 is complete.

In view of Theorem 3. 3, it might seem natural to assume next that (2) is weakly normal. However, the following lemma suggests that a weaker hypothesis is more suitable. (We recall that the square of a weakly normal endomorphism is strongly normal; see [2], Corollary to Theorem 3. 1.)

Lemma 4. 2. *If θ is a semi-normal endomorphism of the loop G, each of the following statements implies the others:*

(i) *θ^2 is a normal endomorphism of G.*

(ii) *The complement, $\lambda = (\theta^2)'$, of θ^2, is a semi-normal endomorphism of G.*

(iii) *θ^2 is a strongly normal endomorphism of G. When* (i), (ii), (iii) *hold, $\theta\lambda$ is a centralizing endomorphism of G.*

Proof. We use the results of [2]. If θ^2 is a normal endomorphism, then λ is a normal (and hence semi-normal) endomorphism. Thus (i) implies (ii). We recall that

$$\theta^2 + \lambda = 1 = \textit{the identity mapping}$$

and hence

$$\theta^3 + \theta\lambda = \theta.$$

If θ is a semi-normal endomorphism, θ^3 and θ coincide on the commutator-associator subloop G'. Therefore $\theta\lambda$ maps G' into 1. If λ is also a semi-normal endomorphism, then $\theta\lambda$ is semi-normal. Since $\theta\lambda$ maps G' into 1, it follows that $\theta\lambda$ is a centralizing endomorphism. Then $\theta^2\lambda$ is also centralizing; and this means that θ^2 is strongly normal. Thus (ii) implies (iii); and, a fortiori, (iii) implies (i). This completes the proof of Lemma 4. 2.

Now, if G is power-associative, then for each integer n, we define the power-mapping (n) of G by

$$x(n) = x^n \tag{4.14}$$

for every x in G.

Lemma 4.3. *Let* (2) *be a semi-normal endomorphism of the loop* G, *and impose one of the following conditions:*

(a) (4) *is a normal endomorphism of* G.

(b) (-3) *is a semi-normal endomorphism of* G.

(c) (3) *is a semi-normal endomorphism of* G.

Then all of (a), (b), (c) *are satisfied. Indeed,* (n) *is a semi-normal endomorphism of* G *for every integer* n. *And more is true:*

(i) *If* $n \equiv 0 \bmod 6$, (n) *is centralizing.*

(ii) *If* $n \equiv 0$ *or* $1 \bmod 3$, (n) *is strongly normal.*

(iii) *If* $n \equiv 2 \bmod 3$, (n) *is normal or strongly normal according as* (2) *is normal or strongly normal.*

(iv) *A necessary and sufficient condition that* (2) *be strongly normal is that* $G^2 \subset Z(G)$, *where* $Z(G)$ *is the centre of* G. *When* (2) *is strongly normal,* (n) *is strongly normal for every integer* n.

(v) *A necessary and sufficient condition that* (2) *be normal is that* $G^2 \subset C(G) \cap Z_2(G)$, *where* $C(G)$ *is the Moufang centre and* $Z_2(G)$ *is the second centre of* G. *When* (2) *is normal,* (n) *is normal for every integer* n.

Proof. Since the complement of (4) is (-3), the conditions (a), (b) are equivalent by Lemma 4.2. In addition, if (a) or (b) holds, $(2)(-3) = (-6)$ is a centralizing endomorphism. In this case, (6) is also a centralizing endomorphism. On the other hand, if (c) holds, then, in view of the identities (4.2), (4.4) of Lemma 4.1, $(6) = (2)(3)$ is again a centralizing endomorphism.

From this point on, we assume that (6) is a centralizing endomorphism. The following equations link together pairs of complementary mappings:

$$1 = (1) + (0) = (4) + (-3) = (3) + (-2) = (2) + (-1); \tag{4.15}$$

$$(1)(0) = 0; \quad (4)(-3) = (-12); \quad (3)(-2) = (-6); \quad (2)(-1) = (-2). \tag{4.16}$$

And the next equations show that certain mappings differ by a centralizing endomorphism:

$$(4) = (-2) + (6); \quad (3) = (-3) + (6); \quad (5) = (-1) + (6). \tag{4.17}$$

If we assume (a) or (b), then (4) and (-3) are strongly normal endomorphisms (by Lemma 4.2). Thus, by (4.17), (3) is also a strongly normal endomorphism. If we assume (c), then, by hypotheses, (3) is a semi-normal endomorphism and hence, by (4.17), (-3) is also a semi-normal endomorphism; that is, (b) holds. Hence (a), (b), (c) are equivalent and we assume all three henceforth. Then, since (4) is strongly normal, (4. 17) shows us that (-2) is also a strongly normal endomorphism.

Since (1) and (4) are (strongly) normal endomorphisms, then, by Theorem 3. 3 and the fact that (2) is a semi-normal endomorphism, $(5)= =(1)+(4)$ is a semi-normal endomorphism. By this and (4. 17), (-1) is a semi-normal endomorphism.

If n is any integer, there exist unique integers m, k such that

$$n=m+6k, \quad m=0, \pm 1, \pm 2, 3. \tag{4.18}$$

We have already seen that (m) is (at least) a semi-normal endomorphism for each admissible choice of m in (4. 18). Moreover, $(6k)$ is a centralizing endomorphism, since (6) is. Therefore

$$(n)=(m)+(6k)$$

is semi-normal, and (n) is normal or strongly normal according as (m) is.

If $n\equiv 0 \bmod 6$, then $m=0$. This proves (i).

If $n\equiv 0$ or $1 \bmod 3$, then $m=0,\ 1,\ -2$ or 3. Since (0), (1), (-2) and (3) are strongly normal endomorphisms, so is (n). This proves (ii).

If $n\equiv 2 \bmod 3$, then $m=-1$ or 2. By (4. 15), (2) and (-1) are complementary; thus if one is a normal or strongly normal endomorphism, so is the other. This proves (iii).

Since (2) and (-1) are complementary and since $(2)(-1)=(-2)$, we see that (2) is strongly normal precisely when (-2) is centralizing. However, (-2) is centralizing precisely when (2) is centralizing. This proves (iv). On the other hand, since (-2) is, in any case, strongly normal, the criterion in [2] shows that (2) will be normal precisely when (-2) maps G into

$$C(G)\cap Z_2(G).$$

Since (2) and (-2) have the same image, this proves (v) and completes the proof of Lemma 4. 3.

Theorem 4. 1. *Let $\mathfrak{N}$ be the set of all normal endomorphisms of the loop G. Then each of the following conditions implies the other two:*

(i) *$\mathfrak{N}$ is an associative ring under addition and multiplication of mappings.*

(ii) *The square-mapping* (2) *is a normal endomorphism of G.*

(iii) *The power-mappings* (2) *and* $(3)=(2)+(1)$ *are semi-normal endomorphisms of G, and* (2) *maps G into $C(G)\cap Z_2(G)$. (Here $C(G)$ is the Moufang centre and $Z_2(G)$ is the second centre of G.)*

When the conditions are satisfied, G is power-associative and $6\mathfrak{N}$ consists of centralizing endomorphisms of G.

Proof. Clearly (i) implies (ii). If (ii) holds, certainly (2) is semi-normal and $(2)^2=(4)$ is normal. By Lemma 4.3, if (2) is a semi-normal endomorphism, then (4) is a normal endomorphism precisely when (3) is a semi-normal endomorphism. Moreover, when (2) and (3) are semi-normal endomorphisms, a necessary and sufficient condition that (2) be normal is that (2) map G into $C(G) \cap Z_2(G)$. Therefore (ii) and (iii) are equivalent.

Next we assume (ii), (iii). Then, by Lemma 4.1, G is power-associative. However, by the main theorem of [3], power-associativity ensures that the additive loop generated by $\mathfrak{N}$ is a ring $\mathfrak{R}$. We wish to show that $\mathfrak{N}$ coincides with $\mathfrak{R}$. Let θ, φ be in $\mathfrak{R}$. By Lemma 4.3, since (2) is normal, so is (-1). Thus the element $\theta - \varphi = \theta + (-1)\varphi$ of $\mathfrak{R}$ is a sum of two elements θ, $(-1)\varphi$ of $\mathfrak{N}$. Hence, by Theorem 3.3, $\theta - \varphi$ is in $\mathfrak{N}$. This shows that $\mathfrak{N}$ is closed under subtraction. Hence, by the definition of $\mathfrak{R}$, $\mathfrak{N} = \mathfrak{R}$. Thus (i) holds. That is, (i), (ii), (iii) are equivalent. When (i), (ii), (iii) hold, Lemma 4.3 tells us that (6) is a centralizing endomorphism. Hence $6\mathfrak{N}$ consists of centralizing endomorphisms, and the proof of Theorem 4.1 is complete.

Theorem 4.2. *Each of the following statements about the loop G implies the other two:*

(i) *The set $\mathfrak{N}'$ of all strongly normal endomorphisms of G is an associative ring under addition and multiplication of mappings. (Moreover, every normal endomorphism of G is strongly normal.)*

(ii) *The square-mapping* (2) *is a strongly normal endomorphism of G.*

(iii) *The square-mapping* (2) *is a centralizing endomorphism of G.*

Proof. Each of (i), (iii) clearly implies (ii). If (ii) holds, then, a fortiori, (2) is a normal endomorphism. Hence, by Theorem 4.1, the set $\mathfrak{N}$ of normal endomorphisms of G is a ring. Moreover, by Lemma 4.3, (iii) is precisely the condition that (2) be strongly normal. Thus (ii) and (iii) are equivalent. To show that (ii), (iii) imply (i), we proceed as follows: If θ is in $\mathfrak{N}$, with complement θ', then $\theta\theta' = \varphi$ where, according to the criterion of [2], φ is a strongly normal endomorphism which maps G into $C(G) \cap Z_2(G)$. Since $C(G)$ is commutative Moufang, (3) induces a centralizing endomorphism of $C(G)$. Thus $3\varphi = \varphi(3)$ is a centralizing endomorphism of G. However, $2\varphi = \varphi(2)$ is a centralizing endomorphism of G, since (2) is. Thus $\varphi = 3\varphi - 2\varphi$ is centralizing, and this means that θ is strongly normal. Hence $\mathfrak{N} = \mathfrak{N}'$. Therefore we have (i). This completes the proof of Theorem 4.2.

If (2) is a centralizing endomorphism of a loop G, then $G^2 = G(2)$ is a normal subloop of G contained in the centre $Z(G)$; and G/G^2 is a loop, say T, of exponent two. We may remark that, although groups of exponent two are abelian groups, no such statement can be made about loops of exponent two. Indeed, the class of all loops of exponent two is a very large — and not too well explored — class containing, for example, the totally symmetric loops. The latter are co-extensive with Steiner triple systems. For various contructions of loops of exponent two, see [4] and [5].

The following construction reduces the study of loops whose strongly normal endomorphisms form a ring to the study of a fairly simple type of central extension:

Construction. Let T be any multiplicative loop of exponent two, let A be any additive abelian group, and let f be any function from $T\times T$ to A satisfying the conditions

$$f(t, 1)=0=f(1, t), \tag{4.19}$$

$$f(tt', tt')+2f(t, t')=f(t, t)+f(t', t') \tag{4.20}$$

for all t, t' in T. Then let $G=(T, A; f)$ be the set of all couples (t, a), $t\in T$, $a\in A$, with equality componentwise and with multiplication defined by

$$(t, a)(t', a')=(tt', f(t, t')+a+a'). \tag{4.21}$$

If we omit (4.20), G is the most general loop such that $G^2\subset Z(G)$ and G/G^2 is homomorphic to T (where G^2 denotes the subloop — here normal in G — generated by all squares). The identity (4.20) is necessary and sufficient in order that the square-mapping of G be a (necessarily centralizing) endomorphism of G.

We shall not dwell on the theory of these central extensions; cf., e. g., [6]. In a similar way we could construct all loops G satisfying the conditions of Theorem 4.1. We first observe that, for such a loop G, $G/Z(G)$ is of the type just constructed, and hence may be obtained from a loop $(T, A; f)$ by a central extension. The conditions which must be imposed, however, are rather forbidding, in contrast to the simple condition (4.20).

5. The general case. It will be convenient to begin with two lemmas:

Lemma 5.1. *Let θ be a normal endomorphism of the loop G, and let φ be an endomorphism of $G\theta$. Let P be any one of the properties (of endomorphisms) of being semi-normal, weakly normal, normal or centralizing. Then $\theta\varphi$ has property P relative to G if and only if φ has property P relative to $G\theta$.*

Remark. The conclusion of Lemma 5.1 becomes false (if the normal endomorphism θ of G is not strongly normal) when P is taken to be the property of being strongly normal — as is clear when we choose φ to be the identity mapping of $G\theta$. This choice of P is treated in Lemma 5.2 below.

Proof. First let P be one of the properties of being semi-normal, weakly normal or normal. Then there exists a class $\mathfrak{K}$ (depending on P; see [2]) of normalized, purely non-abelian loop words such that $\theta\varphi$ has property P relative to G if and only if

$$W_n(x_1\theta\varphi, x_2, \ldots, x_n) = W_n(x_1, x_2, \ldots, x_n)\theta\varphi \tag{5.1}$$

for each W_n in $\mathfrak{K}$ and all $x_1, \ldots, x_n$ in G, whereas φ has property P relative to $G\theta$ if and only if

$$W_n(x_1\theta\varphi, x_2\theta, \ldots, x_n\theta) = W_n(x_1\theta, x_2\theta, \ldots, x_n\theta)\varphi \tag{5.2}$$

for each W_n in $\mathfrak{K}$ and all $x_1, \ldots, x_n$ in G.

If (5.1) holds, we replace $x_2, \ldots, x_n$ by $x_2\theta, \ldots, x_n\theta$, respectively, in (5.1). Then the left-hand side of (5.1) becomes the left-hand side of (5.2), whereas the right-hand side of (5.1) becomes

$$W_n(x_1, x_2\theta, \ldots, x_n\theta)\theta\varphi = W_n(x_1\theta, x_2\theta, \ldots, x_n\theta)\varphi.$$

Thus (5.1) implies (5.2). Conversely, if (5.2) holds, we replace $x_2, \ldots, x_n$ by $x_2\theta, \ldots, x_n\theta$, respectively, in (5.2). Using, the facts that

$$W_n(z, x_2, \ldots, x_n)$$

lies in the commutator-associator subloop G' and that the normal endomorphisms θ and θ^3 coincide on G', we deduce this time that

$$W_n(x_1\theta\varphi, x_2, \ldots, x_n)\theta^2 = W_n(x_1, x_2, \ldots, x_n)\theta\varphi. \tag{5.3}$$

Now we must prove that the left-hand sides of (5.3), (5.1) are equal.

We prove this as follows: Since θ is a normal endomorphism of G, then θ^2 and $\lambda = (\theta^2)'$ are strongly normal endomorphisms of G and $\theta\lambda$ is a centralizing endomorphism of G. (Compare the proof of Lemma 4.2.) If x is in G, then, since φ is an endomorphism of $G\theta$, there exists at least one y in G such that $x\theta\varphi = y\theta$. Hence the element $x\theta\varphi\lambda = y\theta\lambda$ is in the centre of G; that is, the endomorphism $\theta\varphi\lambda$ of G is centralizing. Therefore, if

$$a = W_n(x_1\theta\varphi, x_2, \ldots, x_n),$$

then

$$a\lambda = W_n(x_1\theta\varphi\lambda, x_2\lambda, \ldots, x_n\lambda) = 1$$

and

$$a = a(\theta^2 + \lambda) = (a\theta^2)(a\lambda) = a\theta^2.$$

This proves that (5.3) implies (5.1), and completes the proof that (5.1), (5.2) are equivalent identities.

There remains only the case that P is the property of being centralizing. However, an endomorphism of a loop H is centralizing precisely when it is semi-normal and maps H' into 1. If one of $\theta\varphi$, φ is semi-normal, then both are (by the previous proof). Since, moreover, $G'\theta\varphi=(G\theta)'\varphi$, $\theta\varphi$ maps G' into 1 precisely when φ maps $(G\theta)'$ into 1. This completes the proof of Lemma 5.1.

Lemma 5.2. *If θ is a strongly normal endomorphism of a loop G and if φ is an endomorphism of $G\theta$, then $\theta\varphi$ is a strongly normal endomorphism of G precisely when φ is a strongly normal endomorphism of $G\theta$.*

Proof. Since strongly normal endomorphisms are normal, we may assume, in view of Lemma 5.1, that $\theta\varphi$ and φ are both normal. The element a of G is in G' if and only if $a\theta$ is in $(G\theta)'$. Moreover, since θ is a strongly normal endomorphism of G, $a\theta=a\theta^2$ for every a in G'. Then, for a in G',

$$a(\theta\varphi)\theta=a\theta(\theta\varphi)=a\theta^2\varphi=a\theta\varphi$$

and

$$a(\theta\varphi)^2=(a\theta)\varphi^2.$$

Hence $(\theta\varphi)^2$ coincides with $\theta\varphi$ on G' precisely when φ^2 coincides with φ on $(G\theta)'$. In view of the properties of normal endomorphisms, this is enough to prove Lemma 5.2.

Theorem 5.1. *Let $\mathfrak{N}$ be the set of all normal endomorphisms of the loop G, and let $\mathfrak{S}$ be the set of all θ in $\mathfrak{N}$ such that $2\theta=\theta+\theta$ is in $\mathfrak{N}$. Then $\mathfrak{S}$ is a ring. Moreover:*

(i) $\mathfrak{N}+\mathfrak{S}=\mathfrak{S}+\mathfrak{N}=\mathfrak{N}$;

(ii) $\mathfrak{N}\mathfrak{S}=\mathfrak{S}\mathfrak{N}=\mathfrak{S}$;

(iii) $G^2\mathfrak{S}\subset C(G)\cap Z_2(G)$, *where $C(G)$ is the Moufang centre and $Z_2(G)$ is the second centre of G.*

Proof. By Lemma 5.1, if θ is in $\mathfrak{N}$, a necessary and sufficient condition that $2\theta=\theta+\theta=\theta(2)$ be in $\mathfrak{N}$ is that the square-mapping (2) of G induce a normal endomorphism of $G\theta$. Thus we are led to consider the class $\mathfrak{K}$ of all normal subloops H of G such that the square-mapping (2) of G induces a normal endomorphism of G/H. By Theorem 4.1, the G-normal subloop H will be in $\mathfrak{K}$ if and only if the mappings (2) and (2)+(1) of G induce semi-normal endomorphisms of G/H and, moreover,

$$G^2H/H\subset C(G/H)\cap Z_2(G/H).$$

Using these conditions, it is not hard to see that there exists a finite class, $\mathfrak{L}$, of loop words W_n such that the G-normal subloop H is in $\mathfrak{K}$ if and only if H contains $W_n(x_1, x_2, \ldots, x_n)$ for each W_n in $\mathfrak{L}$ and all $x_1, \ldots, x_n$ in G. Now it should be clear that $\mathfrak{K}$ contains a minimal element, $K=K(G)$. As a consequence, the element θ of $\mathfrak{N}$ is in $\mathfrak{S}$ if and only if $K\theta=1$.

Hereafter, let θ be in $\mathfrak{S}$. By Theorem 4. 1, applied to $G\theta$:

(a) *$G\theta$ is power-associative;*

(b) (-1) *is a normal endomorphism of $G\theta$.*

If φ, ψ are in $\mathfrak{N}$ and x is in G, then

$$(x\theta, x\varphi) = (x, x)\theta\varphi = 1, \quad (x\theta, x\varphi, x\psi) = (x, x, x)\theta\varphi\psi = 1$$

by (a), and hence

$$\theta + \varphi = \varphi + \theta, \quad (\theta + \varphi) + \psi = \theta + (\varphi + \psi).$$

By Theorem 3. 2, if φ is in $\mathfrak{N}$, then $\theta + \varphi = \varphi + \theta$ is in $\mathfrak{N}$ and $\theta\varphi$, $\varphi\theta$ are in $\mathfrak{S}$. This is enough to prove (i), (ii), if we recall that $\mathfrak{N}$ contains the identity mapping of G and note that $\mathfrak{S}$ contains the zero mapping of G. In addition,

$$K(\theta + \varphi) = K\theta \cdot K\varphi = K\varphi,$$

so $\theta + \varphi$ is in $\mathfrak{S}$ precisely when φ is. Hence we see that $\mathfrak{S}$ is closed under an associative and commutative addition. Moreover, by (b) and Lemma 5. 1, $\theta^* = \theta(-1)$ is a normal endomorphism of G. Since θ^*, like θ, maps K upon 1, and since $\theta + \theta^*$ is the zero mapping of G, it is now clear that $\mathfrak{S}$ is an additive abelian group. In view of (ii) and the fact that distributive laws are automatic for endomorphisms, we see finally that $\mathfrak{S}$ is a ring.

Again, $G^2\theta = G\theta(2) \subset C(G\theta) \cap Z_2(G\theta)$, by Theorem 4. 1 applied to $G\theta$. By Lemma 2. 6, for any θ in $\mathfrak{N}$, $G^2\theta \subset C(G\theta)$ is equivalent to $G^2\theta \subset C(G)$. Similarly, by simple calculations using commutators and associators $G^2\theta \subset Z_2(G\theta)$ is equivalent to $G^2\theta \subset Z_2(G)$. This proves (iii) and completes the proof of Theorem 5. 1.

Theorem 5. 2. *Let $\mathfrak{N}'$ be the set of all strongly normal endomorphisms of the loop G, and let $\mathfrak{S}'$ be the set of all θ in $\mathfrak{N}'$ such that $2\theta = \theta + \theta$ is in $\mathfrak{N}'$. Then $\mathfrak{S}'$ is a ring. Moreover:*

(i) $\mathfrak{N}' + \mathfrak{S}' = \mathfrak{S}' + \mathfrak{N}' = \mathfrak{N}'$.

(ii) $\mathfrak{N}'\mathfrak{S}' = \mathfrak{S}'\mathfrak{N}' = \mathfrak{S}'$.

(iii) *The element θ of $\mathfrak{N}'$ is in $\mathfrak{S}'$ if and only if the following two conditions are satisfied:*

$$f_4(x, x, y, y)\theta = 1 \tag{5.4}$$

for all x, y in G, and

$$G^2\theta \subset Z(G), \tag{5.5}$$

where $Z(G)$ is the centre of G.

Proof. Let θ be in $\mathfrak{N}'$. Then, by Lemma 5. 2, $2\theta = \theta(2)$ is a strongly normal endomorphism of G if and only if (2) induces a strongly normal endomorphism of $G\theta$. By Theorem 4.2 applied to $G\theta$, (2) induces a strongly normal endomorphism of $G\theta$ if and only if (2) induces a centralizing endomorphism of $G\theta$. From the definition of f_4, (2) induces an endomorphism of $G\theta$ if and only if (5.4) holds for all x, y in G. And (2) maps $G\theta$ into its centre, $Z(G\theta)$, if and only if $G^2\theta \subset Z(G\theta)$; but, since θ is (in particular) semi-normal, this latter condition is equivalent to (5.5). Therefore we have proved (iii).

If θ is in $\mathfrak{S}'$ and φ is in $\mathfrak{N}'$ then $\theta\varphi$ and $\varphi\theta$ are in $\mathfrak{N}'$ (see [2]). Also (5.4), (5.5) obviously hold with θ replaced by $\theta\varphi$ or $\varphi\theta$. This is enough to prove (ii).

At this point it will be convenient to note that if θ and 2θ are both in $\mathfrak{N}'$, then both are in $\mathfrak{N}$. Hence $\mathfrak{S}'$ is a subset of $\mathfrak{S}$. As a result, if θ is in $\mathfrak{S}'$ and φ in in $\mathfrak{N}'$, then, by Theorem 5.1, $\theta+\varphi=\varphi+\theta$ is in $\mathfrak{N}$. Also, by the preceding paragraph, $\theta\varphi$ and $\varphi\theta$ are in $\mathfrak{S}'$. Again (see [2]), $\theta\varphi$ and $\varphi\theta$ differ by a centralizing endomorphism of G. Since, in addition, $2\theta\varphi$ is a centralizing endomorphism (inasmuch as $\theta\varphi$ is in $\mathfrak{S}'$), we conclude that

$$\theta\varphi+\varphi\theta=\lambda \tag{5.6}$$

where λ is a centralizing endomorphism of G. Again (see [2]), since θ, φ are in $\mathfrak{N}'$,

$$\theta^2=\theta+\mu, \quad \varphi^2=\varphi+\nu \tag{5.7}$$

where μ, ν are centralizing endomorphisms of G. Combining (5.6), (5.7) with the fact that $\theta^2, \theta\varphi, \varphi\theta$ are in $\mathfrak{S}'\subset\mathfrak{S}$, we get

$$\begin{aligned}(\theta+\varphi)^2 &= (\theta+\varphi)\,\theta+(\theta+\varphi)\,\varphi= \\ &=\theta^2+\varphi\theta+\theta\varphi+\varphi^2=\theta+\varphi+\varrho\end{aligned}$$

where $\varrho=\lambda+\mu+\nu$ is a centralizing endomorphism of G. Now it is clear that the element $\theta+\varphi$ of $\mathfrak{N}$ is in fact in $\mathfrak{N}'$. And this is enough to prove (i).

Again let θ be in $\mathfrak{S}'$. Then $G\theta$ is power-associative and $\mathfrak{N}'(G\theta)$ is a ring. In particular, (-1) induces a strongly normal endomorphism of $G\theta$. Consequently, by Lemma 5.2, $\theta^*=\theta(-1)$ is in $\mathfrak{N}'$. Since θ^* clearly satisfies the same conditions (5.4), (5.5) as θ, we see that θ^* is in $\mathfrak{S}'$. Hence $\mathfrak{S}'$ contains the negatives of its elements.

If θ, φ are in $\mathfrak{S}'$ then $\theta+\varphi$ is in $\mathfrak{N}'$ (as shown above). Moreover, since θ and φ satisfy (5.4), (5.5), so does $\theta+\varphi$. Hence $\mathfrak{S}'$ is closed under addition. Now we have that $\mathfrak{S}'$ is an additive subgroup of $\mathfrak{S}$. By this and (ii), $\mathfrak{S}'$ is a subring of $\mathfrak{S}$. And now the proof of Theorem 5.2 is complete.

It will be noted that, in Theorem 5.2, we gave explicit necessary and sufficient conditions that θ be in $\mathfrak{S}'$. It would have been easy, in Theorem

5.1, to give explicit necessary and sufficient conditions that θ be in $\mathfrak{S}$. We refrained from doing so merely because the conditions seemed too space-consuming.

6. Rings generated by normal endomorphisms. Up until this point we have been concerned mainly with rings consisting of normal endomorphisms. Here we indicate some other possibilities by proving the following theorems:

Theorem 6.1. *Let G be a commutative, di-associative loop, let $\mathfrak{N}$ be the set of all normal endomorphisms of G, and let $\mathfrak{N}$ be the additive loop generated by $\mathfrak{N}$ under addition of mappings. Then $\mathfrak{N}$ is a ring of endomorphisms of G.*

Theorem 6.2. *Let G be an arbitrary loop, let $\mathfrak{N}$ be the set of all normal endomorphisms of G, let $\mathfrak{N}^*$ be the set of all θ in $\mathfrak{N}$ such that $G\theta$ is commutative and di-associative, and let $\mathfrak{N}^*$ be the additive loop generated by $\mathfrak{N}^*$ under addition of mappings. Then $\mathfrak{N}^*$ is a ring of endomorphisms of G. Moreover, $\mathfrak{N}\mathfrak{N}^* = \mathfrak{N}^*\mathfrak{N} = \mathfrak{N}^*$.*

Proof. Clearly Theorem 6.1 is a corollary of Theorem 6.2. Hence we need only prove Theorem 6.2. If φ is in $\mathfrak{N}^*$, there exists at least one loop word

$$F_n = F_n(X_1, X_2, \ldots, X_n)$$

and elements $\theta_1, \theta_2, \ldots, \theta_n$ of $\mathfrak{N}^*$ such that

$$\varphi = F_n(\theta_1, \theta_2, \ldots, \theta_n). \tag{6.1}$$

Moreover (compare [3]),

$$x\varphi = F_n(x\theta_1, x\theta_2, \ldots, x\theta_n) \tag{6.2}$$

for each x in G.

From F_n we define a loop word L_{2n} by

$$\begin{aligned} &F_n(X_1Y_1, X_2Y_2, \ldots, X_nY_n) = \\ &= [F_n(X_1, \ldots, X_n)\, F_n(Y_1, \ldots, Y_n)]\, L_{2n}(X_1, \ldots, X_n, Y_1, \ldots, Y_n). \end{aligned} \tag{6.3}$$

Thus L_{2n} is a member of the free multiplicative group on the $2n$ free generators $X_1, \ldots, X_n, Y_1, \ldots, Y_n$. Since L_{2n} obviously vanishes on every abelian group, L_{2n} is purely non-abelian. As a consequence, by the method in [3], L_{2n} can be built up from normalized, purely non-abelian words of form

$$W_{s+t}(X_{i_1}, \ldots, X_{i_s}, Y_{j_1}, \ldots, Y_{j_t}) \tag{6.4}$$

on some but perhaps not all of the $2n$ generators. (Here one of s, t can be zero.) Now let x, y be arbitrary elements of G, and substitute $x\theta_k$ for X_k, $y\theta_k$ for Y_k, $k=1,2,\ldots,n$. From the fact that each θ_k is in $\mathfrak{N}^*$ and hence in $\mathfrak{N}$, we deduce that (6.4) becomes

$$W_{s+t}(x,\ldots,x,y,\ldots,y)\theta_{i_1}\cdots\theta_{i_s}\theta_{j_1}\cdots\theta_{j_t}. \tag{6.5}$$

If θ is the product of endomorphisms appearing in (6.5), then θ is also in $\mathfrak{N}^*$. Hence, since the subloop generated by $x\theta$ and $y\theta$ is an abelian group, (6.5) must be equal to the identity. As a consequence,

$$L_{2n}(x\theta_1,\ldots,x\theta_n,y\theta_1,\ldots,y\theta_n)=1 \tag{6.6}$$

for all x, y in G. In view of (6.2), (6.3), (6.6), we have

$$(xy)\varphi=(x\varphi)(y\varphi)$$

for all x, y in G. This proves that each element φ of $\mathfrak{N}^*$ is an endomorphism of G.

Now let us assume temporarily that G is commutative and di-associative, so that $\mathfrak{N}^*=\mathfrak{N}$ and $\mathfrak{N}^*=\mathfrak{N}$. Since di-associativity implies power-associativity, it follows from the main theorem of [3] that $\mathfrak{N}^*=\mathfrak{N}$ is a ring. This completes the proof of Theorem 6.1.

In the general case of Theorem 6.2, we still have to prove that $\mathfrak{N}^*$ is a ring. As a first step, we must show that the additive loop $A=(\mathfrak{N}^*,+)$ of $\mathfrak{N}^*$ is an abelian group. For this it is enough to show that if φ, given by (6.1), is in the commutator-associator subloop A' of A, then $\varphi=0$. However, if φ is in A', we can always suppose that F_n is in the commutator-associator subloop of the free loop on $X_1,\ldots,X_n$. This means that F_n is purely non-abelian. But then, by a simplication of the proof of (6.6) — this time using only power-associativity — we get (cf. [3])

$$x\varphi=F_n(x\theta_1,\ldots,x\theta_n)=1$$

for all x in G. This means that A is an abelian group.

Next let $\theta_1,\ldots,\theta_n$ be arbitrary elements of $\mathfrak{N}^*$, let φ be any element of $\mathfrak{N}^*$, given by (6.1), and let θ be any element of $\mathfrak{N}$. Then, using (6.2), we see that

$$\theta\varphi=F_n(\theta\theta_1,\ldots,\theta\theta_n),\quad \varphi\theta=F_n(\theta_1\theta,\ldots,\theta_n\theta).$$

In addition, all of the products $\theta\theta_i$, $\theta_i\theta$ are easily seen to be in $\mathfrak{N}^*$. This is enough to prove that $\mathfrak{N}\mathfrak{N}^*=\mathfrak{N}^*\mathfrak{N}=\mathfrak{N}^*$. In particular, $\mathfrak{N}^*\mathfrak{N}^*\subset\mathfrak{N}^*$. Next, for any fixed φ in $\mathfrak{N}^*$, let $\mathfrak{M}$ be the set of all ψ in $\mathfrak{N}^*$ such that $\psi\varphi$ is in $\mathfrak{N}^*$. We see readily that $\mathfrak{M}$ is an additive subgroup of $\mathfrak{N}^*$; hence $\mathfrak{M}=\mathfrak{N}^*$. Therefore $\mathfrak{N}^*$ is closed under multiplication. Since $\mathfrak{N}^*$ consists wholly of endomorphisms, the distributive laws are automatic. Hence $\mathfrak{N}^*$ is a ring, and the proof of Theorem 6.2 is complete.

Bibliography

[1] R. H. Bruck, A Survey of Binary Systems, *Ergebnisse der Math. und ihrer Grenzgebiete*, Neue Folge, Heft **20** (Berlin—Göttingen—Heidelberg, 1958).

[2] ——— Normal endomorphisms, *Illinois Journal of Math.*, **4** (1960), 38—87.

[3] ——— Sums of normal endomorphisms, *Proc. Amer. Math. Soc.*, **10** (1959), 674—678.

[4] ——— Some results in the theory of quasigroups, *Transaction Amer. Math. Soc.*, **55** (1944), 19—52.

[5] ——— What is a loop? (In press; to appear in a volume published by the *Math. Assoc. of America.*)

[6] ——— An extension theory for a certain class of loops, *Bull. Amer. Math. Soc.*, **57** (1951), 11—26.

UNIVERSITY OF WISCONSIN,
MADISON, WISCONSIN, U. S. A.

(Received March 22, 1960)